图书情报工作
ChinaXiv合作期刊
第65卷 第9期 2021年5月

可信电子文件证据效力保障技术方案研究*

■ 许晓彤[1,2] 侯景瑞[3]
[1] 山东大学历史文化学院 济南 250100 [2] 中国人民大学电子文件管理研究中心 北京 100872
[3] 武汉大学信息管理学院 武汉 430072

摘 要：[目的/意义]立足于电子文件管理与电子证据应用的跨学科视角，提出维护可信电子文件证据效力的技术方案。[方法/过程]系统分析司法认可的各项真实性保障技术的原理、优势与尚待解决的问题，归纳并提出"电子签名+时间戳""区块链辅助真实性验证"和"电子文件－电子证据全区块链管理"3类可信电子文件证据效力保障技术方案，分析其适用性并规划对应的管理流程。[结果/结论]3类技术方案能够支持不同组织机构根据电子文件的应诉需求、格式、密级等因素综合部署相关管理工作，显著提升电子文件的证据效力保障的效能。

关键词：可信电子文件 证据效力 技术方案 电子文件管理
分类号：G275
DOI：10.13266/j.issn.0252－3116.2021.09.004

随着新基建、智慧社会、工业4.0的快速发展，云计算、物联网、区块链与人工智能等技术迅速渗透各行各业，生产生活全面趋向网络化、信息化与数据化。可信的信息、文件与数据作为构建数字信任机制的基本单元，成为维护和促进数字社会生态发展的关键。在学理上，"电子系统中文件真实性永久保障国际合作项目(The International Research on Permanent Authentic Records in Electronic Systems，InterPARES)"将文件的可信性(trustworthiness of a record)的判断标准定义为真实性、可靠性与准确性[1]；在实践中，电子文件的可信性则体现在能否成为业务活动的凭证，实现机构内部、机构间乃至司法层面的认可。当前，《中华人民共和国电子签名法》(下文简称《电子签名法》)、《计算机犯罪现场勘验与电子证据检查规则》《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》《最高人民法院关于互联网法院审理案件若干问题的规定》等法律文件陆续明确规定了司法认可的电子证据真实性保障技术，将是否应用电子签名、电子认证、可信时间戳、哈希(Hash)值校验、区块链等技术作为电子证据真实性审查判断的要点之一。在证据自生成到最终采信的时间链上，电子文件管理是电子证据的"前端控制"环节，电子证据则是电子文件管理的"后端应用"之一[2]；在流通性较强、应诉概率较高的电子文件管理工作中有选择、有计划地对标司法需求配置技术方案，有助于维护电子文件的证据效力，使其在应对纠纷与诉讼风险时具备证明力优势，提升机构间乃至社会层面的信任效率。

1 国内外相关研究情况

由于法系和立法进程差异，国内外对电子文件证据效力保障技术的研究侧重点各不相同。1982年，欧洲理事会秘书长在《电子处理资金划拨》报告中提出计算机记录可以相当于书面文件作为证据[3]，英美法系国家陆续通过调适电子证据对传闻规则、最佳证据规则与鉴证规则等证据规则的适用，明确了电子证据的可采性。具体而言，一方面，关注文件是否"由正常的日常业务活动制作、形成"(Record Made in the Usual and Ordinary Course of Business)[4-5]；另一方面，关注电子文件及系统的完整性，如加拿大《统一电子证据法》通过审查电子文件及其存储系统在各关键时刻均处于

* 本文系教育部规划基金项目"数字保存的成本计量与控制研究"(项目编号：20YJA870018)、山东省社会科学规划项目"基于区块链技术的可信文档数据治理生态建设研究"(项目编号：21DTQJ01)和国家档案局科技项目"区块链技术在电子档案单套制管理中的应用研究"研究成果之一。
作者简介：许晓彤(ORCID：0000－0002－2900－3796)，助理研究员，博士，E-mail：xuxiaotong@sdu.edu.cn；侯景瑞(ORCID：0000－0002－7234－3200)，硕士研究生。
收稿日期：2020－12－21 修回日期：2021－02－08 本文起止页码：32－40 本文责任编辑：易飞

正常运行状态推定该文件具备完整性、可以采纳[6]。英美法系中对电子文件证据效力的关注多从信息系统的视角通盘考虑,如美国国家标准 ANSI/AIIM TR31《法律可接受的信息系统生成记录》(Legal Acceptance of Records Produced by Information Technology Systems)规定了信息系统生成记录的基本要求与自我评估;加拿大国家标准 CAN/CGSB-72.34《电子文件用作书证》(Electronic Records as Documentary Evidence)对电子文件作为法律证据的要求与整体文件管理方案作出规定,阐释了电子签名与物理签名的配合使用等[7]。此外,国外学者还将数字取证(Digital forensics)技术运用到电子文件管理中,辅助实现电子文件的可靠捕获与传输、检测伪造或非授权行为等[8]。如 J. L. John 将数字取证的部分技术手段前置于电子文件管理的业务流程中[9];"数字文件取证"(Digital Records Forensics,DRF)项目则构建了能够与电子文件管理衔接的数字取证功能模型[10];C. Lee 则开发可用于图书馆、档案馆数字管护实践的数字取证技术工具 BitCurator,辅助符合法律规格要求的数字资源的形成、提取与展示利用等[11]。

我国于 2004 年颁布了《电子签名法》,明确了数据电文的法律证据效力,在纸质文件占据主流的当时,薛四新等[12]、王艳明[13]等学者积极探索电子签名技术在电子文件管理系统中的应用路径,将其视作维护电子文件法律效力的有力手段,文件与档案管理领域开始集中关注与研究电子签名技术。直至 2012 年,电子证据作为第八大证据类型正式确立了在三大诉讼法中的法定地位,相关法律法规快速增长。据笔者在北大法宝、北大法意数据库的检索与通读,截至 2021 年 2 月 4 日,对电子证据收集保全与审查判断作出详细规定的法律文件已达 14 部。受电子证据整体立法进程的影响,此前的电子文件管理技术研究与司法可采性的交融有限,但学者们从文件与档案管理的视角对下列几类电子文件真实性保障技术进行了研究:①电子签名技术。如前所述,《电子签名法》的颁布引发了文件与档案管理领域对电子签名技术的研究热情;随着电子签名技术在实践工作中的广泛应用,电子签名的归档处置问题受到关注[14-15]。②数字水印技术。研究数字水印技术的种类与特点[16],分析其对档案原始性的保护作用及其应用前景[17]等。③时间戳技术。探讨了可信时间戳在电子档案移交、备份、长期保存等环节的应用[18],设计了基于可信时间戳的电子档案取证与验证的具体方案[19]等。④区块链技术。近三年来,区块链技术成为热点,其在文档管理场景中的应用前景[20-21]、基于区块链技术的电子文件存储方案[22]、系统模型[23]、文档管理可信生态[24]等问题受到关注。此外,赵屹对文件固化、哈希校验、数字签名、可信时间戳、区块链等技术的防篡改原理进行了专门研究,着重分析了其对文档管理工作的影响与启示[25]。

总结上述成果,从研究视角来看,国外电子文件管理技术方面的相关研究与司法证据互动交融频繁;而我国相关法律规定的制定多集中于近几年内,以往的研究多从文件与档案管理本领域的需求出发,与司法证据用途结合较少。从研究内容来看,当前我国对电子文件真实性保障技术的研究多侧重技术的原理解释与应用意义分析,或针对某个具体的管理场景展开研究,对多重技术的综合性研究比较有限。基于此,本文立足于电子文件管理与电子证据应用的跨学科视角,以证据效力维护为目标,对司法认可的电子签名、电子认证、可信时间戳、哈希值校验、区块链等真实性保障技术的原理与特征进行系统分析,探索适配不同类型机构电子文件证据效力保障的技术方案,为电子文件实现机构内、机构间以及社会层面的可信生成、可信流转、可信共享与可信存储提供参考,为行业技术的规范化应用与数字信任生态建设奠定基础。

2 司法认可的电子文件真实性保障技术对比分析

为更有针对性地部署可信电子文件证据效力保障的技术方案,需厘清各项司法认可真实性保障技术的原理,阐明其应用于电子文件管理的优势、特色与尚待解决的问题。

2.1 司法认可的电子文件真实性保障技术

根据各项法律文件的规定,司法认可的真实性保障技术有哈希值校验、电子签名、电子认证、可信时间戳、区块链。现分别对其技术原理进行简要分析。

2.1.1 哈希校验技术

哈希校验是基于哈希函数运算的一种真实性保障技术,其原理是通过一个散列函数或哈希表映射,将不定长的字符串或其他类型数据转换成固定长度的数字串输出[26]。当电子文件发生任何变化,其哈希值也随之变化,亦无法通过哈希值倒推电子文件的变动情况,这种不可逆的特性是哈希算法用于防篡改和身份认证的关键所在。一般输出长度越长,该哈希算法越安全。目前国际上较为常用的哈希算法有 SHA-1(160bit)、

MD5(128bit)等,SHA－1 的变体 SHA－256 还可输出 256bit 长度的哈希值[27],我国对标 SHA－256 的国密 SM3 也是目前安全性较高的一种主流算法。

2.1.2 电子签名与电子认证技术

根据《电子签名法》的定义,电子签名(Electronic signature)指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据,其最常见的实现方式是数字签名(Digital signature),即用非对称密钥加密技术制成的电子签名[28],需运用公开密钥算法和前文所述的哈希算法。如无特别说明,本文所述电子签名均为数字签名。发送方使用自己的私钥对信息(通常是电子文件的哈希值)进行签名,接收方使用发送方公开的公钥验证签名,确保信息来自于发送者本人,实现其不可抵赖性。电子认证(Electronic authentication)在法律意义上是指专门的、具有资质的认证机构(Certificate Authority,CA)对电子签名及其持有者身份进行真实性验证的法律服务[29],形成第三方对发信人身份的担保;在技术实现层面则指的是以电子认证证书(又称数字证书,Digital certificate)为核心的加密技术,它以 PKI(Public key infrastructure,公钥基础设施)为基础,对网络传输的信息进行加密、解密、签名与验签[30]。虽然法律文件将电子签名、电子认证并列为两种电子证据真实性保障技术,但二者应当是相伴相生的:电子签名主要解决了验证信息是否被更改的问题,电子认证进一步确认通信伙伴是否为本人的问题;电子签名可直接应用于封闭型、交互型的系统中,而开放型网络则需要电子认证的第三方保障;电子签名是技术层面的保障,电子认证是包含组织、技术、基础设施等的复杂系统或过程。

2.1.3 时间戳技术

如前所述,电子签名能够有效解决电子文件的伪造、篡改和身份假冒等问题,但在确认制作时间方面,时间戳技术(Time-stamp)更具优势,这对于电子证据的真实性审查和证据链的形成具有重要意义。在我国,受法律认可的时间戳特指中国科学院国家授时中心联合信任时间戳服务中心(NTSC UniTrust Time Stamp Authority,TSA)提供的“可信时间戳”服务。时间戳文件包括电子文件的哈希值、时间戳服务机构收到哈希值的日期与时间、时间戳服务机构的签名 3 个部分,其工作原理与电子签名和电子认证基本一致,能够证明电子文件从特定的时间点开始直至被验证时不曾被篡改,可看作包含时间信息的电子签名。

2.1.4 区块链技术

区块链(Blockchain)是一种多方共同维护,应用密码学保证传输与访问安全,实现数据一致存储、难篡改、防抵赖的记账技术,也称为分布式账本技术(Distributed ledger technology)[31]。它并不是一种“新”技术或单项技术,而是分布式存储、共识机制、点对点传输、加密算法等技术在互联网时代的创新应用模式[20,32]。顾名思义,“区块链”的特点在于将数据区块以链式结构组织并存储,这是其实现防篡改的关键。在区块链上,每一个区块由区块头和区块体组成,区块头包含记录区块封装时间的时间戳与 Merkle 根哈希值,区块体则按需记录电子文件的哈希值等数据信息。Merkle 根哈希值是区块体中以 Merkle 树叶子节点存储的数据两两哈希运算生成的总哈希值,区块体中任何的数据变化均会引起 Merkle 根哈希值的变动。各区块通过哈希指针连接并按顺序在时间轴上链式分布,某一区块数据的变动将引发其后所有区块头中的哈希值改变,数据一旦写入便不可篡改。区块链技术将电子文件的内容与形成时间、顺序牢牢地绑定在一起,维护了数据整体的真实性、完整性与可追溯性。

2.2 各项技术综合比较与分析

通过前文的具体分析可知,各项真实性保障技术的作用原理与功能并非彼此独立,而是相互关联、不断发展。哈希校验是实现防篡改验证的核心,在此基础上发展出了电子签名与电子认证技术、时间戳技术,前者在防篡改的基础上能够识别文件形成者数字身份的有效性,后者则实现了权威时间信息的确认;当前许多数字签名或时间戳产品已集成了这两项技术的共同优势,实现了身份权属与制作时间的同步确认。而区块链技术可基于前述三类技术与智能合约、共识机制等技术,实现无需权威第三方的信任。

上述技术推广应用至电子文件管理实践中时亦具备不同的优势与尚待解决的问题:

哈希校验的防篡改机制使其成为一系列真实性保障技术的基础,为电子文件的真实性提供了简捷、高效的证明方式。且哈希函数的算法公开、透明,哈希值的生成与验证几乎“零成本”实现,使用门槛较低。但哈希校验的效果较为单一,部门间或机构间开展业务时还需要实现对电子文件权属与形成时间的确认,这就需要通过电子签名与电子认证、时间戳技术加以实现。

电子签名与电子认证在电子文件证据效力的保障方面具有一定优势:一方面,有利于实现内容的防篡改,通过对比即时哈希值与加签原始哈希值的一致性,

许晓彤，侯景瑞. 可信电子文件证据效力保障技术方案研究[J]. 图书情报工作,2021,65(9):32－40.

有助于确认电子文件内容是否完好无损；另一方面，有利于确保行为的不可抵赖，CA 机构为电子文件发送者的公钥和私钥的唯一对应性背书，只要私钥未经泄露，即可确定该电子文件的签署者，排除身份假冒的可能性，辅助电子证据认定中对“人”与“事”关联性的判断。但同时，电子签名与电子认证的局限性亦十分明显：在效率与成本方面，摘要形成、加解密、签名验签等环节的增加一定程度上影响了现有电子文件管理流程的运行效率，CA 机构的服务成本也带来了客观阻碍；在后续处置方面，电子签名是否归档、如何归档尚无定论，目前我国的 CA 机构有 30 余家，采用不同 CA 机构服务时亦可能产生信任冲突[33]，且实践工作中还面临着由于 CA 机构关停、脱离原生软硬件环境、算法失效或数字证书撤销等原因导致无法验证，或电子文件迁移过程中无法成功迁移电子签名信息等问题[14]，进一步影响了电子签名的稳定性与时效性。

时间戳技术在电子文件证据效力保障中的核心优势亦基于哈希算法的单向不可逆性，能够确保电子文件未被篡改。同时，相比于一般的电子签名，可信时间戳技术为电子文件添加了权威、可信、安全的时间信息，且目前国内权威的时间服务机构仅一家，避免了争议的发生，有助于确定电子文件的形成、制作时间，辅助形成可信的证据链条。此外，可信时间戳具有价格优势，如其对电子数据认证的价位是每条 10 元，批量使用则更为经济[34]。然而在准确定位电子文件与签名人的身份方面，由于一般组织机构在购买可信时间戳服务接口与管理员权限后，机构内部的时间戳使用权限靠管理员进行人工分配，具体分配情况可能不是一一对应的关系，需对操作痕迹进行排查，这在一定程度上降低了确定电子文件权属的效率。

区块链技术在电子文件证据效力保障方面具备独特优势：一方面，区块链技术实现了新型信任机制，其无中心机构、无中心系统、无第三方背书、依靠共识机制运行的模式使区块链上的信息可“自证真实”，实现了以人和权威机构为中心的信任机制向基于逻辑和代码信任机制的转变[35]；另一方面，智能合约满足条件即自动触发的机制有助于减少人为干预的不确定因素，维护证据保管链条的完整性。尽管区块链技术在防篡改方面具有明显优势，但由于尚属于新兴技术，行业规范和标准较为缺乏，应用于可信电子文件的管理还存在一系列问题：首先，区块链的不可更改性在赋予其维护真实性技术优势的同时也为电子文件管理流程带来了挑战，即记录的更改必须重新生成区块，且难以删除；其次，由于区块链系统覆盖了固化、长期保存、真实性保障等功能，削弱了归档、鉴定等环节的必要性[20]，难以与电子文件管理系统衔接调适，可能影响机构的业务开展流程；再次，区块链技术仅能保障“链上真实”，电子文件如不能实现形成即上链，仍需通过其他手段证明其在链下的可靠性；最后，区块链为维护数据安全，需执行大量无意义的计算，因而面临运行效率与成本投入等客观困难，英国区块链电子档案信任管理项目 ARCHANGEL 为提升效率，仅将电子文件与相关元数据的哈希值上链[36]。但若实现基于智能合约的全自动管理，则对区块链各节点的基础设施与经济投入提出了更高的要求，需要组织机构本身具有较强的“链改”意愿与决心。

综上，各项技术在防篡改机制、功能、成本、效率等方面各有其优势，应用于电子文件管理时也存在一定问题（详见表 1）。据此，可从电子文件管理场景需求出发，将相关技术组合形成“互补”技术方案，以发挥其最大优势、规避可能发生的问题与风险。

表 1　司法认可的真实性保障技术在可信电子文件证据效力保障中的应用效果比较分析

技术类型	优势与特点	待解决的问题
哈希校验技术	①不可逆、防篡改； ②成本低廉	①部分算法安全性较低； ②效果单一
电子签名与电子认证技术	①哈希校验防篡改； ②将签署人与电子文件绑定，行为不可抵赖； ③有 CA 机构第三方背书	①CA 机构间或存在信任冲突； ②是否/如何归档保存仍有争议； ③效率与成本问题客观存在
时间戳技术	①哈希校验防篡改； ②确认电子文件形成与管理时间； ③价格较低； ④有唯一服务机构权威背书	确认文件权属的效率有待提升
区块链技术	①块链式结构防篡改； ②无需第三方背书的去中心化信任机制； ③智能合约解决对人为操作的不信任问题	①内容修改较为不便； ②与电子文件系统的衔接问题； ③无法根本解决内容可靠性问题； ④资源、效率与成本问题客观存在

3　电子文件证据效力保障技术方案设计及适用性分析

从维护电子文件可信性、保障电子文件证据效力的视角出发，前文所述各项技术均具备保证电子文件在无反驳证据的情况下认定真实的能力。因而，组织机构可基于对各项技术特点的分析，结合自身业务需求与文档管理实际条件选择适用的技术或技术组合方

案,避免因过度使用技术导致不必要的成本投入与资源浪费,造成机制协调与运行效率风险。证据效力保障技术方案的设计与选择应充分考量前端业务开展的方式与实际需要,即关注电子文件管理中的“前驱”[37]因素;结合前文对各项司法认可的真实性保障技术优势与特性的分析,本文归纳了“电子签名 + 时间戳”“区块链辅助真实性验证”和“电子文件 – 电子证据全区块链管理”3 类电子文件证据效力保障技术方案,它们分别在不同时间点以不同形式介入电子文件的生命周期,适用于不同类型的电子文件管理场景。

3.1 方案一:“电子签名 + 时间戳”

一般地,电子文件由各类业务系统形成,被人工归档或自动捕获至文件与档案管理系统并长久保存;同时,系统自动生成描述上述管理过程的元数据。在此基础上,电子签名技术和时间戳技术配合形成了十分稳定的真实性保障技术组合,能够实现对电子文件权属与制作时间的确认,该方案在实践工作中已得到了较为广泛的应用与验证。如薛四新[38]提出的“电子文件身份证”构想,它通过对电子文件核心元数据、电子文件实体和电子文件哈希值进行语义计算,融合得出属于该电子文件的唯一身份标识,与电子文件生成单位添加的数字签名和时间戳共同封装。“电子签名 + 时间戳”技术方案的重点在于:①应用电子签名技术和时间戳技术的时间节点越早越好,应提前至业务办理环节,固化其内容与形成时间;②应将电子文件及其元数据、电子签名、时间戳共同封装为归档信息包,作为真实性保障技术的使用凭证,以备审计或需要诉讼时形成时间轴证据链。

该技术方案应用较为普遍、成本投入明确,与一般电子文件管理工作的流程与逻辑适配度高,可用于管理具备应诉需求与应诉风险的电子文件,并向电子文件管理制度体系完整、管理流程与系统规范、管理能力处于平均水平的机构推行。

3.2 方案二:“区块链辅助真实性验证”

随着区块链技术的广泛应用,中国石油化工集团有限公司(简称中石化)、中国科学院合肥分院等部分机构已将区块链技术引入文档管理场景,用于电子文件的长久可信保存。“区块链辅助真实性验证”是一种“链上 + 链下”的技术方案,其形成流转阶段与方案一一致,但需在归档信息包形成后即时计算其哈希值,并将归档信息包与哈希值分别存入数字档案馆系统与区块链系统。一旦发生应诉时,可重新计算电子文件归档信息包的哈希值,并将其与区块链上存储的哈希值进行对比,结果一致即可证明电子文件未经篡改。此方案的核心在于利用区块链技术的防篡改“自证”属性,解决组织机构间电子文件管理工作的不信任,或不同 CA 机构间不信任等问题。但需要指出的是,该方案在归档环节才开始应用区块链技术辅助哈希值存证,仅能证明上链后未经篡改。2021 年 1 月,最高人民法院最新颁布的《关于人民法院在线办理案件若干问题的规定(征求意见稿)》中也明确指出,如当事人提出数据上链存证时已不具备真实性,举证方还应就上链存证数据的具体来源、生成机制、存储过程、第三方公证见证、关联印证数据等情况作出补充说明。因此,方案二的实施前提在于电子文件上链前管理的合规性。但整体而言,以区块链辅助真实性验证不失为一种可靠的技术方案,有利于电子文件证明力的提升。

对于一般组织机构而言,“区块链辅助真实性验证”的方案在现有电子文件管理工作秩序的基础上,为其证据效力保障锦上添花,易于推广实施;且由于区块链对上链格式有固定要求,区块的大小固定、可扩展性有限[39],本方案可辅助非结构化或容量较大的电子文件的哈希值上链管理;此外,仅将哈希值上链,有利于电子文件内容信息的保密、防止泄密风险发生。对于部分具备法律效力并需要在业务办理环节发挥相应职能的电子文件而言,仅从归档环节上链仍有风险。建议有分布式存储条件或区块链应用需求的组织机构以此方案进行过渡与试点,逐步向更全面的区块链应用探索。

3.3 方案三:电子文件 – 电子证据全区块链管理

如前所述,数据一旦登入无法篡改的特性使区块链技术具有“自证”真实的功能。方案三的关键在于使电子文件形成、管理与长期保存的全过程上链,并接入司法区块链,以司法机关的见证实现电子文件 – 电子证据全链条的防篡改、可追溯。此外,区块链技术的另一个核心功能在于智能合约,“一旦满足条件则自动触发”的机制亦契合了电子证据审查认定中关于“电子证据是否为系统自动发送”的判断标准。目前,针对电子邮件、电子合同、设计文件等应诉率较高的电子文件类型,网易、百度、存证云、联合信任时间戳等公司纷纷推出了“公正邮”“电子签”“微版权”等涉及各领域的电子存证服务产品,其中部分产品与公证、鉴定机构直接合作,能够实现有应诉需求时“一键出证”。上述服务通过互联网实现业务的“形成即固化”与“形成即上链”,以形式真实确保内容可靠,证明电子文件自形成起至收集并提交法庭之前未经篡改。电子文件 – 电子证据全区块链管理的前提是业务环节上链,首先需

要组织机构根据自身需求选择底层区块链技术方案，搭建业务环境和文档管理环境，并在业务环节时就将电子文件转化为能够在区块链系统中流通的“虚拟资产”通证(Token)，通过对Token的管理实现对电子文件的管理；其次，需将电子文件管理归档、鉴定、处置等相关规则写入智能合约，并将智能合约预置于区块链系统中，实现自动化操作，如设置执行定期脱链存储的时间期限等。此外，为满足部分电子文件的高应诉需求，有条件的机构可申请加入司法机关建设的联盟链，实现电子文件与数据在应诉中的直接验证与实时调用，使电子文件向电子证据的转化更为便利。如北京互联网法院相继颁布了《天平链应用接入管理规范》和《天平链应用接入技术规范》，为外部系统接入天平链提供了详细指引，有助于全面构建基于区块链的可信生态。

相较于前两种技术方案，电子文件-电子证据全区块链管理能够最大程度地发挥区块链技术的优势，但对现有业务秩序的影响较大、前期投入与后期维护成本较高，难以在短时间内推广至各类电子文件管理工作中。但对于金融财税、知识产权等对电子文件真实性保障较为敏感、应诉需求较高的领域，可率先选取电子合同、电子发票等本身就具备一定法律效力的、结构化的电子文件类型进行试点。一旦该管理模式应用于各行业领域中，其带来的生产效能与经济效益、节省的时间与成本将十分可观，亦能避免不必要的诉讼与纠纷的发生。

3.4 各类技术方案综合比较与分析

在司法证据认定中，对证据保管链(Chain of custody)完整性的审查是必要环节，它要求证据保管者对证据流转和安置过程及其相关保管人员的沿革情况完全记录并负相应责任[40]，这与电子文件管理中强调的全生命周期管理有异曲同工之妙。从这一视角看，方案一中使用的电子签名与时间戳确认了电子文件形成时的权属与时间，结合参考2019年《最高人民法院关于民事诉讼证据的若干规定》第九十四条中关于“以档案管理方式保管的电子数据可在无反驳证据的情况下认定真实性”的规定，归档后的电子文件具备证明力优势。因此，方案一能够实现电子文件全生命周期的真实性认证，但前提在于使用具有专业资质开发商开发的、符合国家与行业标准的管理系统，保证电子文件管理与存储环境的清洁性，便于确认电子文件与元数据符合档案管理的要求。方案二中区块链技术的使用时机在归档之时，因而一般可与方案一结合使用，补充对电子文件形成阶段的真实性证明。方案三实现了电子文件的全生命周期上链，并与司法区块链联通，能够实现电子文件-电子证据全流程真实性见证。三类方案各具优势与特色，可适用于不同类型的电子文件与不同类型的组织机构，具体如表2所示：

表2 三类技术方案综合对比

技术方案	实施时机	证据效力保障机理	适用电子文件特征	适用机构类型
方案一：基本模式	形成办理过程中	电子文件办理时添加电子签名并与时间戳一同归档；可通过验证电子签名和时间戳的有效性以及电子文件管理系统的资质确认电子文件的证据效力	一般有应诉需求与应诉风险的电子文件均适用	电子文件管理制度体系完整、管理流程与系统规范、管理能力处于平均水平的机构
方案二：区块链辅助真实性验证	归档管理时	将归档电子文件及相关信息的哈希值存储在区块链上；可通过对比即时计算哈希值与链上存储哈希值的异同确认电子文件的证据效力	有应诉需求与应诉风险的电子文件；非结构化或容量较大的电子文件；密级较高或含有隐私信息的电子文件	有一定分布式存储条件与区块链应用需求的组织机构
方案三：电子文件-电子证据全区块链管理	链上同步形成	电子文件全程形成流转于区块链平台，可对接司法区块链，有应诉需求时可直接调用	应诉需求与应诉风险高的电子文件；结构化的电子文件	涉及高应诉概率业务、具备区块链系统部署条件的组织机构

4 基于多重技术方案的可信电子文件证据效力保障流程实现

前文探讨的3类证据效力保障技术方案介入电子文件生命周期的时机、形式各不相同，但其真实性保障机理亦存在相通之处；其管理流程既有区别，也有交叉。实践中，电子文件管理工作可能对接多重业务，面临多样化的证据效力保障需求，需同时采用多种技术方案；或需要分步、分批地推进不同技术方案。为更加直观地体现多重技术方案所对应管理流程的区别与联系，本文将对其进行综合阐释，详见图1。

如图1所示，假设组织机构配置有办公自动化系统、核心业务系统、财务系统等多类业务系统(Business System，下文简称BS)，BS-1、BS-2与BS-3这3类业务系统分别生成适用于前述方案一、方案二与方案三的电子文件类型；本示例方案中部署的区块链系统类型为联盟链。

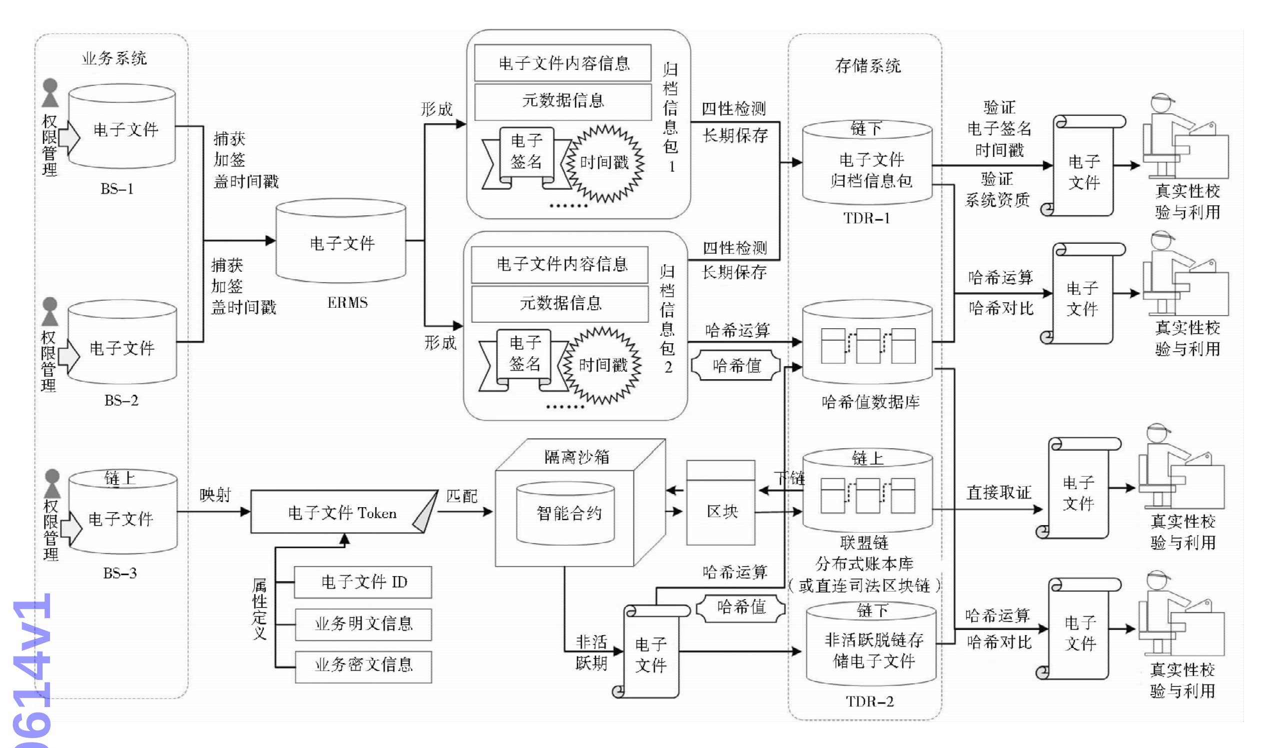


图 1　基于多重证据效力保障技术方案的可信电子文件管理流程示例

BS－1 生成的电子文件在添加电子签名与时间戳信息后被电子文件管理系统（Electronic Records Management System，下文简称 ERMS）捕获，与相关元数据一起封装形成归档信息包 1，对其进行四性检测并将其长期保存在数字档案馆系统（Trusted Digital Repositories，下文简称 TDR）中。当电子文件面临出证需求时，可验证其电子签名、时间戳的有效性与系统资质的可靠性，通过验证的电子文件即可执行出证利用。以上管理流程完全在本地系统加以实现。实践中，苏大苏航数据保全中心的档案数据保全核心思路与本方案类似：保全中心接收归档数据包后执行四性检测，计算其哈希值并添加可信时间戳；同时，数据包将被制作 3 套备份存储于不同的服务器中长期保存。当用户需调阅数据时，将重新计算归档数据包的哈希值并与接收时的哈希值进行比对，结果一致即可证明保全过程中未经篡改。由于数据保全中心的业务范围并不涉及文件的形成流转，无需再额外添加电子签名确认数据权属，仅使用可信时间戳作为确认电子文件自接收起未经篡改的证明即可。

BS－2 生成的电子文件在归档保存之前的管理流程与 BS－1 一致，但归档前还需对归档信息包进行哈希运算，将哈希值存储在区块链上的哈希值数据库中，电子文件及其他信息组成的归档信息包仍保存于链下的 TDR－1 内。当电子文件面临出证需求时，可对存储于 TDR－1 中的归档信息包进行哈希运算，并将哈希值与区块链上存储的哈希值进行对比，对比一致即可执行出证利用。以上管理流程的形成与存储阶段均依靠本地系统实现，哈希值的归档保存则在区块链系统中实现。该方案为目前电子文件管理领域应用区块链技术最常采用的方案之一。如中石化档案区块链为解决跨机构信任问题，将跨机构形成或调阅电子文件的特征信息与元数据的哈希值存储在区块链平台上，原始的电子文件按照原要求保存[41]；四川省大竹县某机构在办公自动化平台归档时将电子文件哈希值同步存入当地综合档案馆的区块链系统，实现了全生命周期追踪。上述两所机构均表示未来计划实现电子文件全生命周期上链，并探索管理其他业务区块链上文件的策略，这也与本文方案三的核心思路一致。

BS－3 中的电子文件以 Token 的形式流转，如一份电子合同、一份电子保单等。用户可向 Token 添加属性并视情况决定是否使用电子签名为数据权属背书，一般的、可在联盟链节点机构共享的业务信息可以明文形式添加，对于敏感的、保密的信息如身份证号、电话号码等可实施脱敏加密，还可添加电子文件登记号等。同时，智能合约被提前安装在区块链系统中，可实现对通证的管理，使其自动执行登记、归档、销毁等活动，并将形成的新区块存储在联盟链分布式账本库中。此外，为应对直接存储通证属性信息带来的数据冗余，可定期将链上电子文件脱链存储。具体地，可根据相关规定在智能合约中设置脱链周期，电子文件脱

链进入本地存储时同时生成哈希值,使哈希值进入相应的数据库长期保存。例如对于疫苗的接收、购进、储存、配送、供应的相关记录,根据《中华人民共和国疫苗管理法》的规定,需保存至疫苗有效期满后不少于5年备查[42],则可将脱链保存周期设置为5年或以上。面临出证利用需求时,BS－3的流程与BS－2一致。目前,方案三尚属理论构想,但随着区块链技术的深入发展,如交通银行"链交融"证券系统、阿里健康区块链等基于区块链的业务平台将逐步增加。可以预见,电子文件－电子证据全区块链管理这一模式有望在未来得到更广泛的应用。

综上,组织机构可全面梳理各类业务系统产生的电子文件的性质、结构类型、应诉需求与保密需要,充分评估其电子文件管理能力、基础设施条件与资金投入水平,在本机构电子文件管理工作规划的指导下选择一种或多种适用的技术方案,并将其实现流程整合在已有业务流程与管理秩序之中,以实现可信电子文件证据效力保障的最佳效能。

5 结论与展望

通过前文对司法认可的电子文件真实性保障技术机理的研究及技术方案的探讨,可知3种技术方案在保障电子文件的证据效力、辅助司法证据的认定方面各有特色。虽然区块链技术"自证"真实的特性具有先天优势,无需依赖其他权威机构便可实现"自我背书",避免了第三方风险;但若采用资质齐备的电子文件管理系统以及合法的电子认证与时间戳服务,亦能完成真实性的认证。从这一角度来说,机构的电子文件管理工作无需过度、重复采用相关真实性保障技术或一味追求新兴技术,无论是在现有管理秩序的基础上增加电子签名与时间戳,还是部署覆盖至业务端的区块链系统,均能够在各自的凭证价值证明体系中合理自洽。且技术方案仅作为维护电子文件内容与管理痕迹可信的保障性手段,管理哪些、何时管理、如何管理等方案与策略的部署才是电子文件证据效力保障的关键。因而,组织机构在选择技术方案时,应以电子文件证据效力保障的最佳效能为目标,充分考量本机构的文档管理基础、业务工作需要、人员配备与资金配置等多重因素,重点关注文件本身是否具备法律属性、应诉需求大小、保密需要、在数字化转型中是否急需等关键问题,在此基础上作出综合决策。随着技术的发展和业务环境的变革,电子文件管理积极探索与区块链等新兴技术的结合将是不可逆转的趋势,后续关于业务系统、电子文件管理系统与区块链系统的协同与融合、电子文件"上链"与"下链"管理的策略等一系列落地性问题还需要学界与业界的深入研究与共同探索。

参考文献:

[1] DURANTI L, PRESTON R. International research on permanent authentic records in electronic systems 2: experiential, interactive and dynamic records [M/OL]. [2020－10－23]. http://www.interpares.org/ip2/display_file.cfmdoc=ip2_book_complete.pdf.
[2] 许晓彤,肖秋会. 电子文件与证据法学中相关概念的比较及其演化脉络分析[J]. 档案学通讯,2019(2):23－28.
[3] 刘品新. 论电子证据的定位——基于中国现行证据法律的思辨[J]. 法商研究,2002(4):37－44.
[4] 沈达明. 英美证据法[M]. 北京:对外经济贸易大学出版社,2015.
[5] Canada evidence act[EB/OL]. [2021－02－01]. https://laws-lois.justice.gc.ca/PDF/C-5.pdf.
[6] 何家弘,刘品新. 电子证据法研究[M]. 北京:法律出版社,2002.
[7] Electronic records as documentary evidence[EB/OL]. [2021－02－01]. https://www.scc.ca/en/standardsdb/standards/28933.
[8] Digital Preservation Coalition. Digital preservation handbook[EB/OL]. [2021－02－01]. https://www.dpconline.org/handbook/technical-solutions-and-tools/digital-forensics.
[9] JOHN J L. Digital forensics and preservation[M]. Salisbury: Charles Beagrie Ltd., 2012.
[10] Digital records forensics project. Digital forensics function model [R/OL]. [2021－02－01]. http://www.digitalrecordsforensics.org/display_file.cfm? doc=drf_conduct_digital_forensics_function_model.pdf.
[11] LEE C. Archival application of digital forensics methods for authenticity, description and access provision[J]. Comma, 2012(2): 133－140.
[12] 薛四新,王建明,王玉. 解读《电子签名法》,思考电子文件归档[J]. 档案学研究,2005(3):54－57.
[13] 王艳明.《电子签名法》对电子文件管理的若干影响[J]. 档案学研究,2006(1):43－46.
[14] 蔡盈芳. 电子文件归档中电子签名的处理研究[J]. 档案学研究,2019(4):103－108.
[15] 刘越男,杨建梁,张洋洋. 单轨制背景下电子签名的归档保存方案研究[J]. 档案学通讯,2019(3):26－35.
[16] 席亚兰. 数字档案的安全维护与数字水印技术[J]. 档案,2006(5):44－45.
[17] 张建明. 数字水印在数字档案馆的应用前景[J]. 浙江档案,2005(1):19－20.
[18] 杨茜雅,赵勇刚. 可信时间戳构筑电子档案安全堡垒[J]. 档案与建设,2013(7):19－22.
[19] 余亚荣,张照余. 基于可信时间戳服务的电子档案证据取证和验证方案设计[J]. 档案管理,2020(1):66－68.
[20] 刘越男. 区块链技术在文件档案管理中的应用初探[J]. 浙江档案,2018(5):7－11.

[21] 张珊. 区块链技术在电子档案管理中的适用性和应用展望[J]. 档案管理,2017(3):18-19.
[22] 石进,薛四新,赵小柯. 基于区块链技术的电子文件真实性保障系统模型研究[J]. 图书情报知识,2019(6):111-119.
[23] 蔡盈芳. 电子档案管理应用区块链存储方式探析[J]. 档案学研究,2020(4):104-109.
[24] 王平,李沐妍,刘晓春. 区块链视角下文件档案管理可信生态的构建[J]. 档案学研究,2020(4):115-121.
[25] 赵屹. 电子文件真实性保障技术发展对档案管理的影响及启示[J]. 档案学研究,2019(6):77-85.
[26] 韩红旗. 语义指纹著者姓名消歧理论及应用[M]. 北京:科学技术文献出版社, 2018.
[27] 梁兴琦. 电子商务安全保密技术及应用,[M]. 合肥:合肥工业大学出版社, 2006.
[28] 赵振洲. 信息安全管理与应用[M]. 北京:中国财富出版社, 2015.
[29] 李守良. 电子商务概论[M]. 郑州:河南科学技术出版社, 2008.
[30] 韩颖梅, 王爽. 电子商务法规[M]. 北京:中国铁道出版社, 2016.
[31] 中国信息通信研究院. 区块链白皮书(2019)[EB/OL]. [2020-11-05]. http://www.cbdio.com/image/site2/20191111/f42853157e261f3346263b.pdf.
[32] 工业和信息化部. 2016 中国区块链技术和应用发展白皮书[EB/OL].[2020-11-18]. http://www.199it.com/archives/526865.html.
[33] 第十届"中国电子文件管理论坛"超隆重开场! 开幕式、十周年庆典、主报告! 火速呈现! [EB/OL]. [2021-04-01]. https://www.sohu.com/a/360417972_734807.
[34] 可信时间戳服务[EB/OL]. [2020-11-14]. http://www.tsa.cn/html/kxsjcfw/.
[35] 区块链如何解决信任机制? [EB/OL]. [2020-11-18]. https://blog.csdn.net/QianZhaoVic/article/details/88771934.
[36] 杨茜茜. 基于区块链技术的电子档案信任管理模式探析:英国ARCHANGEL项目的启示[J]. 档案学研究,2019(3):135-140.
[37] 冯惠玲,刘越男,马林青. 文件管理的数字转型:关键要素识别与推进策略分析[J]. 档案学通讯,2017(3):4-11.
[38] 薛四新. 云计算环境下电子文件管理的实现机理[M]. 上海:世界图书出版公司, 2013.
[39] 中国区块链技术和产业发展论坛. 区块链数据格式规范[EB/OL]. [2020-11-26]. https://blog.csdn.net/wxb880114/article/details/79255631.
[40] GARNER B A. Black's law dictionary[M]. Minnesota:Thomson West, 2014.
[41] 李春艳,乔超. 区块链技术在大型企业集团电子文件管理中的应用——以中国石化为例[J]. 档案学通讯,2020(1):13-20.
[42] 中华人民共和国疫苗管理法[EB/OL]. [2020-12-18]. http://www.npc.gov.cn/npc/c30834/201907/11447c85e05840b9b12c62b5b645fe9d.shtml.

作者贡献说明:

许晓彤:论文选题、撰写、修改;
侯景瑞:参与论文修改。

Study on the Technical Schemes of Evidence Effectiveness Guaranteeing of Trusted Electronic Records

Xu Xiaotong[1,2] Hou Jingrui[3]
[1] School of History and Culture, Shandong University, Jinan 250100
[2] Electronic Records Management Research Center of Renmin University of China, Beijing 100872
[3] School of Information Management, Wuhan University, Wuhan 430072

Abstract: [**Purpose/significance**] Based on the interdisciplinary perspective of electronic records management and electronic evidence application, the technical schemes which aim to maintain the evidence effectiveness of trusted electronic records are proposed. [**Method/process**] This paper demonstrated the authenticity protection mechanism, advantages and unresolved problems of tamper-proof technologies recognized by the judiciary. And three technical schemes for ensuring the evidence effectiveness of trusted electronic records were proposed: "Electronic Signature and Time-stamp" "Blockchain Assisted Authenticity Verification" "Electronic Records-Electronic Evidence Full Blockchain Management", their applicable scenarios and management processes were discussed respectively. [**Result/conclusion**] The technical schemes support various organizations to deploy the work of electronic records management according to the legal requirements, formats, and confidentiality level, which improve the efficiency of evidence effectiveness guaranteeing of the electronic records.

Keywords: trusted electronic records evidence effectiveness technical schemes electronic records management